LECTURE NOTES ON LOCAL FIELDS

PETE L. CLARK

1. Prefatory Comments: June 2009

These notes were originally written to accompany two(?) lectures given in a seminar course led by Barry Mazur at Harvard University in the Fall of 1999. As I write these comments it is summer of 2009. So, whereas I was 23 when the notes were originally written, now I am almost 33: a big difference, mathematically!

The most obvious change in the intervening decade is that then I used a version of LaTex with a command – "run without stopping" – that forced it to compile even in the presence of errors. This was exceptionally bad training, and I find that any document I wrote from this period requires a few minutes per page of error correction.

In this case, I have corrected the Texnical errors. Also I have corrected some mathematical errors that I found – which were mercifully slight. Overall my 23 year-old mathematical self bears a closer resemblance to the current model than I might have expected (good news or bad?). If I would say something different today, I make a brief comment about it, but I have made no attempt to systematically update the notes. In fact I think they hold up well enough for their intended purpose: a first introduction to the structure of local fields.

2. Discrete Valuation Rings

Proposition 1. *Let A be a ring (commutative with unit, as always). TFAE:*
a) A is a domain with field of fractions K, and there is a surjective group homomorphism $v : K^\times \to \mathbb{Z}$, with $v(0) := +\infty$ and $v(x + y) \geq \min\{v(x), v(y)\}$ for all $x, y \in K$ such that A is recovered as $\{x \in K \mid v(x) \geq 0\}$.
b) A is a Noetherian, integrally closed domain with a unique nonzero prime ideal.
c) A is a local PID which is not a field.
d) A is Noetherian local with maximal ideal $m_A = \pi A$, π a non-nilpotent element.
e) There is a non-nilpotent element π of A such that every a in A has a unique expression $a = u\pi^n, u \in A^\times, n \in \mathbb{N}$.
f) A is regular local of dim. 1 (nonzero primes are maximal, $\dim_{A/m} m/m^2 = 1$).
g) A is a local Dedekind ring.
If the above conditions are satisfied we say A is a ***discrete valuation ring*** *(DVR).*

Proof. This is a standard result. See [Serre, Ch. 1], [Atiyah-Macdonald, Ch. 9].[1] □

[1] For a proof of this and other results about discrete valuation rings, see also my notes on Commutative Algebra. –PLC2009

The map in $a)$ is called a **discrete valuation of K**. It's easy to see that $A^\times = \{x \in K \mid v(x) = 0\}$, that $\mathfrak{m} = \{x \in K | v(x) \geq 1\}$ and that π is a generator of the ideal $\mathfrak{m}$ if and only if $v(\pi) = 1$. An element π with $v(\pi) = 1$ is called a **uniformizer** (or **uniformizing element**, or **local parameter**).[2]

The terminology comes from algebraic geometry: if P is a point on a [projective] algebraic curve C, then the ring $K[C]_P \subset K(C)$ of all functions regular at P is a one-dimensional local ring. Using Proposition 1f) above, we see that P is a smooth point if and only if $K[C]_P$ is a DVR. So in this case a local parameter is a rational function f on C regular at P and such that any other rational function regular at P is, up to a unit, a power of f.

Finally, as for any local ring $(A, \mathfrak{m})$, we associate the **residue field** $k = A/\mathfrak{m}$.

Condition g) in Proposition 1 furnishes us with many examples of DVR's: take a Dedekind ring R and localize at any nonzero prime. E.g.:

a) Taking $R = \mathbb{Z}$, then for any prime ideal (p), $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} \mid (p, b) = 1\}$ is a DVR. Here the valuation v is just the familiar function ord_p. The prime p is a uniformizer, and the residue field is $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$.
b) Let K be a number field. Let $R = \mathcal{O}_K$ be the integral closure of $\mathbb{Z}$ in K, so $\mathcal{O}_K$ is a Dedekind ring (e.g. [Serre, 1.4]). Let $\mathcal{P}$ be any nonzero prime of $\mathcal{O}_K$. Then the localization $D_\mathcal{P}$ is a DVR, and using unique factorization of ideals into primes, we get that the valuation ring is precisely (0 and) those elements α of $K^\times$ such that the exponent of $\mathcal{P}$ in the factorization $(\alpha) = \prod_\mathcal{Q} \mathcal{Q}^{ord_\mathcal{Q}(\alpha)}$ is non-negative. The residue field $R_\mathcal{P}/\mathcal{P}R_\mathcal{P} = R/\mathcal{P}$ is a finite extension of $\mathbb{F}_p$, hence a finite field $\mathbb{F}_q$, where $q = p^f$ and f is a divisor of $[K : \mathbb{Q}]$.

c) Let F be any field, and put $R = F[t]$ – a PID, hence *a fortiori* a Dedekind ring. Given any irreducible polynomial $f \in R$, the localization $F[t]_{(f)}$ is as above a DVR. In particular, take $f = t$, so that the valuation map v measures the order of vanishing of a rational function $r(t)$ at $t = 0$. The valuation ring consists of rational functions regular at zero (i.e. the local ring of the affine variety $\mathbb{A}^1_F$ at the origin), and the residue field is canonically isomorphic to F (via evaluation at 0).

3. Completions

There are two routes to completion of a DVR: we can start with the ring or we can start with the fraction field. We recall each in turn.

Algebraic approach: For any Noetherian local ring A we can form the completion $\hat{A} := \varprojlim A/m_A^n$. By standard commutative algebra [Atiyah-Macdonald, Ch. 10], $\hat{A}$ is again a Noetherian local ring with $\mathfrak{m}_A \hat{A} = \mathfrak{m}_{\hat{A}}$. Since by Krull's theorem $\bigcap_n m_A^n = 0$, the natural map $A \to \hat{A}$ is a monomorphism. If we assume

[2] The uniformizer π is far from unique: indeed the set of all uniformizers is a torsor for the group $A^\times$, which is necessarily infinite. –PLC2009

that A is moreover a DVR, then $\mathfrak{m}_A = \pi A \implies \mathfrak{m}_{\hat{A}} = \pi\hat{A}$. Since $A \hookrightarrow \hat{A}$, π remains non-nilpotent, so Proposition 1 applies to show that $\hat{A}$ is a complete DVR. We take K and $\hat{K}$ to be the quotient fields of A and $\hat{A}$ respectively.

Topological approach: Alternately, we can start with the quotient field K. Using the valuation map $v : (K^\times, 0) \to (\mathbb{Z}, \infty)$ we can exponeniate to obtain an *absolute value*: take $c \in (1, \infty)$ and put $||x|| := c^{-v(x)}$. One checks immediately that the new function has the following properties: $|| \; || : K \to [0, \infty)$, $||x|| = 0$ if and only if $x = 0$; $||xy|| = ||x|| \; ||y||$; and $||x + y|| \leq \max\{||x||, ||y||\}$. This last is the so-called **ultrametric inequality** (or **non-Archimedean triangle inequality**). Putting $d(x, y) := ||x - y||$ gives K the structure of a metric space compatible with the field operations.

Take $\hat{K}$ to be the completion of K with respect to the metric d. It's easy to check that $\hat{K}$ retains the structure of a field. (Briefly, let R be the ring of Cauchy sequences in K, $M := \{\text{sequences converging to zero}\}$. Observe that M is a maximal ideal of R and put $\hat{K} = R/M$.) One checks easily that the norm $|| \; ||$ extends continuously to $\hat{K}$, hence the valuation extends to a discrete valuation $\hat{v}$ on $\hat{K}$, i.e. K lies densely in $\hat{K}$ as a valued field. As above, we recover $\hat{A}$ as $\{x \in K^\times \mid ||x|| \leq 1\}$ or better yet,[3] as $\{x \in K | \{x^j\}_{j \in \mathbb{N}} \text{ is bounded}\}$. Similarly,

$$\hat{\mathfrak{m}} = \{x \in K \mid ||x|| < 1\} = \{x \in K \mid x^j \to 0\}.$$

Ostensibly the second approach gives more: a metric topology on $\hat{A}$ and on $\hat{K}$. But recall that there is also a topology associated to completions: we make A into a topological ring by using the ideals m_A^n as a local base at 0; then $\hat{A}$ gets the inverse limit topology with respect to the discrete topology on the quotients A/m_A^n. A little thought shows these are the same topologies defined above.

Examples:

1) $\mathbb{Z}_{(p)}$ is *not* complete. For example, the Baire Category Theorem shows that a complete metric space without isolated points is uncountable. Alternately, use the fact that every integer has a finite base-p expansion to see directly that not every element of the inverse limit comes from an integer. Its completion is isomorphic to the completion of $\mathbb{Z}$ with respect to (p) (since $\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^n\mathbb{Z}$), i.e. $\widehat{\mathbb{Z}_{(p)}} = \mathbb{Z}_p$, the p-adic integers, with quotient field $\mathbb{Q}_p$. Similarly, if K is a number field with a prime ideal $\mathcal{P}$, then $\hat{K} = K_{\mathcal{P}}$ is a finite extension of $\mathbb{Q}_p$. (Sketch proof: Write $K = \mathbb{Q}[\alpha]$ and consider the subfield of $K_{\mathcal{P}}$ generated by $\mathbb{Q}_p$ and α. It contains K and is therefore dense in $K_{\mathcal{P}}$. On the other hand, it is a finite dimensional vector space over $\mathbb{Q}_p$, hence a locally compact subgroup, hence closed in $K_{\mathcal{P}}$.) Note that in either case, the associated complete DVR $\hat{A} = \varprojlim D/m^n$ is an inverse limit of *finite sets*, i.e. a profinite ring; in particular, it is compact. Since $\hat{A}$ is an open neighborhood of 0,this shows that $\hat{K}$, the completion of a number field at a prime ideal, is *locally compact.* Note also that we have an isomorphism of residue fields $\hat{A}/\hat{m} \cong A/m \cong \mathbb{F}_q$, so the residue field is finite.

[3] Why is this better? –PCL2009

2) Take $K = F(t)$ with the valuation v = order of vanishing at 0. Again K is not complete; its completion $\hat{K}$ is the field $F((t))$ of formal Laurent series, with valuation ring $\hat{A} = F[[t]]$. If F is finite, then $F[[t]]$ is profinite in the v-adic topology, and conversely.

4. Local Fields

Fussing about terminology: We will call a field K that is complete with respect to a discrete valuation a **complete field**; e.g., parts I and II of [Serre] deal mostly with arbitrary complete fields. However, this is a rather large class of fields: in particular, [Serre, 2.5] shows that there is a complete field with any given perfect residue field of prime characteristic.[4] On the other hand, the fields $K_{\mathcal{P}}$ and $\mathbb{F}_q((t))$ we considered above had two additional salutary properties: they are locally compact in the valuation topology, and the residue field is finite. In fact among complete fields this is just one salutary property.[5]

Proposition 2. *Let K be a discretely valued field. The following are equivalent:*[6] *a) K is locally compact. b) K is complete with finite residue field.*

Proof. We claim that K is locally compact if and only if A, the valuation ring, is compact. Since A is an open (hence also closed) subgroup of K, the "if" direction is obvious. Conversely, the valuation topology is ultrametric, so a neighborhood base at zero is given by open balls which are also closed. Thus, if there is any compact neigborhood of zero, some ball must be compact; but all open balls in K are homeomorphic via multiplication by π^l for suitable l in $\mathbb{Z}$, so if any ball is compact, so is the unit ball, i.e. the valuation ring A. The result now follows easily: K is complete if and only if A is complete, so A compact implies K complete. The maximal ideal m_A is an open subgroup, so A/m_A is always discrete, so if A is compact, the residue field A/m_A is compact and discrete, hence finite. Finally, if A/m_A is finite, so is A/m_A^n for any n, and if A is complete, $A \cong \varprojlim A/m_A^n$ is profinite, hence compact, so K is locally compact. □

In general, I would like to call a complete valued field with finite residue field a *local field*. Indeed, it turns out that every local field is of the form given in our two examples, namely $\mathbb{F}_q((t))$ or a finite extension of $\mathbb{Q}_p$.

It is quite easy to see that a local field K of chracteristic 0 is a finite extension of $\mathbb{Q}_p$, and we sketch the proof: we have $\mathbb{Q} \hookrightarrow K$. If we consider $v|\mathbb{Q}$ we see that $v(\mathbb{Q}^\times)$ is a discrete subgroup of $\mathbb{Z}$. Moreover this subgroup is nontrivial, for if v is identically zero on $\mathbb{Q}^\times$, $\mathbb{Q}$ is a discrete, hence closed subgroup. But on the other hand $v^{-1}(0) = A^\times$ is a compact subgroup, hence so is $\mathbb{Q}$, giving a contradiction. It's easy to check that any nontrivial discrete valuation on $\mathbb{Q}$ can be renormalized

[4] This is a strange remark, since above we constructed a complete field with any given field F as a residue field: $F((t))$. Probably I meant "a complete field of characteristic zero..." which points towards Witt vectors. – PLC2009

[5] This language is now a bit florid for my taste. –PLC2009

[6] Note that according to our setup, the map $v_0 : K^\times \mapsto 1,\ 0 \mapsto 0$ is not a valuation, since it is not surjective onto $\mathbb{Z}$. Without this convention, every field would become a locally compact field with respect to the valuation v_0, with the induced topology being the discrete one. –PLC2009

to give a p-adic valuation, so $\mathbb{Q}$ with the p-adic topology sits inside K. By functorality of the completion process, the closure of $\mathbb{Q}$ in K is isomorphic to $\mathbb{Q}_p$, so K is a vector space over the field $\mathbb{Q}_p$, which, being locally compact by assumption, must be finite-dimensional.)

For a detailed proof, including the positive characteristic case, see [Ramakrishnan-Valenza, 4.2].

5. Extensions of Local Fields

Theorem 3. *Let K be a local field and L/K a finite field extension. Then there is a unique local field structure on L that extends that of K, i.e. so that the topology of L restricts to give the given (valuation) topology of K.*

Proof. Let A be the valuation ring of K and B be the integral closure of A in L. Being the closure of a Dedekind ring in a finite field extension, B is also Dedekind (see [Serre], [Janusz])). Let $\mathcal{P}$ be a (nonzero) prime of B. Then $\mathcal{P}\cap A$ is a prime of A. Choosing a nonzero element α of $\mathcal{P}$, $N_{L/K}(\alpha)$ is a nonzero element of $\mathcal{P}\cap A$. Since A is a DVR, the only possibility is that $\mathcal{P}\cap A = m_A$. (On the other hand, note that the going-up theorem asserts the existence of at least one such prime.) Now assume there are two primes $\mathcal{P}, \mathcal{Q}$ which lie over m_A. Using the $\mathcal{P}$-adic valuation, we get a topology on L compatible with that of K. But since L/K is a finite dimensional vector space over a complete field, there is a unique vector space topology for L, namely the product topology. Hence the $v_{\mathcal{P}}$-adic and $v_{\mathcal{Q}}$-adic topologies must coincide. Since we can recover the prime $\mathcal{P}$ from the topology as $\{\alpha \in K | \ \alpha_n \to 0\}$, we conclude $\mathcal{P} = \mathcal{Q}$. In particular B is a local Dedekind domain, hence by Proposition 1) a DVR. □

Let L/K be a finite Galois extension of local fields with Galois group G. Since L is a finite-dimensional vector space over K, every element s of G is a K-linear map – necessarily continuous – and hence defines a homeomorphism of G. It follows that every automorphism s preserves both the valuation ring B of L and the maximal ideal m_B, since both can be characterized topologically. Hence s induces an automorphism $\overline{s}$ on $B/m_B =: l$, a finite field which is an extension of $k := A/m_A$. Putting $g := G(l/k)$, we observe that since the automorphism $\overline{s}$ of l fixes A, hence k, pointwise, $\overline{s}$ is an element of g. That is, passage to the quotient gives a group homomorphism $G \to g$. Write $\mathcal{I}$ for the kernel of this map; it is called the **inertia group** of L/K. We have the following basic result.

Theorem 4. *The map $G \to g$ is surjective, i.e. we have an exact sequence*

$$0 \longrightarrow \mathcal{I} \longrightarrow G \longrightarrow g \longrightarrow 0.$$

Proof. Since l/k is Galois, we can write $l = k[\overline{b}]$ for suitable $\overline{b} \in l$. Consider the set $\overline{b_1}, \dots, \overline{b_f}$ of conjugates of $\overline{b}$ over k, on which g acts simply transitively. Now lift $\overline{b}$ to $b \in B$, and let $P_b(t)$ be the minimal polynomial of b over A. It is of the form $\prod_{s\in S\subseteq G}(t-s(b))$, where S is a subset of automorphisms of G that acts simply transitively on the conjugates of b in K. Write $\overline{P}_b(t)$ for the reduction of $P_b(t)$ modulo m_B. Clearly $\overline{P}_b(\overline{b}) = 0$. Since $\overline{P}_b(t) \in k[t]$, it follows that any k-conjugate of $\overline{b}$ is also a root of $\overline{P}_b(t)$; that is, for all $\sigma \in g$, there is $s \in G$ such that $\sigma(\overline{b}) = \overline{s(b)}$. Since $\overline{b}$ generates l/k, $\overline{s} = \sigma$ and $G \to g$ is surjective. □

It is common to write $e := \#\mathcal{I}$, the **ramification index** and $f := \#g$, the **residual degree**. The exact sequence gives us the immediate corollary:

Corollary 5. *We have $[L : K] = ef$.*

If $e = 1$ we say the extension is **unramified**, whereas if $f = 1$ we say it is **totally ramified**. Recall that for any finite separable extension of Dedekind domains B/A and $\mathcal{P}/p$ a prime of B lying over a prime of A we put $e_{\mathcal{P}} := v_{\mathcal{P}}(pB)$, $f_{\mathcal{P}} := [B/\mathcal{P} : A/p]$ and obtain the formula $[L : K] = \Sigma_{\mathcal{P}/p} e_{\mathcal{P}} f_{\mathcal{P}}$ (see e.g. [Serre, Proposition 1.10]). Applying this formula in the case of a local field, it reads $[L : K] = e_{m_B} f$. Thus $e_{m_B} = e = \#\mathcal{I}$.

Finally, we relate the local ($\mathcal{P}$-adic) and global (number field) cases as follows.

Theorem 6. *Let L/K be a degree n extension of number fields, v a discrete valuation of K with valuation ring A, and B the integral closure of A in L. Let $w_1, \ldots, w_r$ be the various extensions of v to a discrete valuation of L, with corresponding indices e_i, f_i as defined above. Let K_v, L_{w_i} be the various completions.*
a) $[L_{w_i} : K_v] = e_i f_i$.
b) w_i is the unique valuation of L_{w_i} extending v, and $e_i = e(L_{w_i}/K_v), f_i = f(L_{w_i}/K_v)$.

Proof. Part a) follows immediately from b) and from Corollary 5, so we need only consider b). On the other hand, b) will follow immediately from Theorem 3, once we verify that L_{w_i} is indeed a finite extension of K_v. Indeed, if $L = K[\alpha]$, then arguing as in Example 1 of Section 1, we see that $L_{w_i} = K_v[\alpha]$. □

Recall that in the global case – L/K an extension of number fields, A the ring of K-integers, B the ring of L-integers, P a prime of B lying over a prime p of A – that elements of the Galois group $G = G(L/K)$ do not in general preserve P. We define the **decomposition group** $D(P/p) := \{s \in G | \ sP = P\}$. We saw that in the local case, the Galois group was "all decomposition," since $sm_B = m_B$ for all s in G. We complete our comparison of local versus global extensions by showing that "localization picks off the decomposition group":

Corollary 7. *If L/K is a Galois extension of number fields with P/p an extension of prime ideals (i.e., the p-adic topology on K is induced by the P-adic topology on L), then $G(L_P/K_p) \cong D(P/p)$.*

Proof. Let s be an element of $D(P/p)$. Viewing L as a dense subfield of L_P, the assumption that $sP = P$ implies that $s(m_B^n) = m_B^n$ for all n, so s is norm-preserving, i.e. an isometry of L. By functorality of completion, s extends uniquely to an isometry of L_P which is easily seen to be an element of $G(L_P/K_p)$. Thus we have defined an injection $D(P/p) \hookrightarrow G(L_p/K_p)$. But both groups have order $e_P f_P$, so the map must be an isomorphism. □

(Remark: Nowadays I would wish to add something about the positive characteristic case and the complications which occur if the residue field is imperfect. –PLC2009)

6. Roots of Unity in Local Fields

In this section we analyze the structure of the group of roots of unity in a local field, in preparation for the following section on unramified extensions.

We introduce the following notation: for K any field and n a positive integer, we write $\mu_n(K)$ for the group of nth roots of unity in K; moreover, we write $\mu'_n(K)$ for the group of roots of unity of K of order *coprime* to n.

Now let K be a local field with residue field $k = \mathbb{F}_q$, $q = p^r$. Then $k^\times$ is a cyclic group consisting of $(q-1)$st roots of unity. Applying Hensel's Lemma to the polynomial $x^{q-1} - 1$, we can lift each element α of $k^\times$ to a root of unity $\tilde{\alpha}$ of K. This gives $q-1$ distinct elements of $\mu_{q-1}(K)$, so these must indeed be all the $q-1$st roots of unity, which implies that the lifting map is unique. In turn this implies that the reduction homomorphism $A^\times \to (A/m)^\times = k^\times$ becomes an isomorphism when restricted to $\mu_{q-1}(K)$. The inverse map $s : (A/m)^\times \to \mu_{q-1}(K) \subseteq A^\times \subseteq K^\times$ is called a *section* of $k^\times$ and the images of the elements of $k^\times$ are called the *multplicative representatives* of $k^\times$ in $A^\times$. (Compare with [Serre, Section 2.4], where this construction is done in more generality.) We abbreviate $\mu'(K) := \mu_{p'}(K)$, the roots of unity of order coprime to the residue characteristic. Clearly we have $\mu_{q-1}(K) \hookrightarrow \mu'(K)$. The principal goal of this section is to show that this map is an isomorphism.

Lemma 8. *For any a in A, $\omega(a) := \lim_{n\to\infty} a^{q^n}$ exists, where $q = p^r = \#A/m$. Moreover, $\omega(a) = 0$ if and only if $a \in m_A$, $\omega(a) = 1$ if and only if $a \equiv 1$ (m_A), and $\omega(ab) = \omega(a)\omega(b)$. It follows that ω induces a homomorphism $\omega : (A/m)^\times \to A^\times$. Indeed, the image lies in $\mu_{q-1}(K)$.*

Proof. First we show that the limit exists. If $a \in m$, clearly $a^{q^n} \to 0$ (and conversely, $a^{q^n} \to 0$ implies $a \in m$), so consider the case of $a \in A^\times$. Using the fact that $p \in m$, one checks easily that $(1+m)^{p^n} \subseteq 1+m^{n+1}$. Since $\#(A/m)^\times = q-1$, $a^{q-1} \in 1+m$, so $a^{(q-1)(q^n)} \in 1 + m^{n+1}$. Putting $\alpha_{n+1} := a^{q^{n+1}} - a^{q^n}$, we get that $\alpha_{n+1} = a^{q^n}(a^{(q-1)q^n} - 1) \in m^{n+1}$, so $\alpha_n \to 0$. Note that since $\lim_{n\to\infty} a^{q^n} = (\Sigma_{n=1}^{\infty}\alpha_n) + a$, the non-Archimedean Cauchy property implies the convergence of the right hand side, hence also of the left hand side. It follows that $\omega(a)$ is well-defined. We saw above that $\omega(a) = 0$ if and only if $a \in m$; and the identity $\omega(ab) = \omega(a)\omega(b)$ is obvious from the definition of ω. Assume now that $a \in 1 + m$; then by the above $a^{p^n} \in 1 + m^{n+1}$, and we conclude that $\omega(a) = 1$. Conversely, if $\omega(a) = 1$, then for sufficiently large m, $a^{q^n} \equiv 1 \pmod{m}$, so $(a-1)^{q^n} \in m$. But m is prime, so $a - 1 \in m$, verifying that $\omega^{-1}(1) = 1 + m$. Thus ω defines a monomorphism $(A/m)^\times = A^\times/(1+m) \to A^\times$. Finally, for $a \in A^\times$, $a^{q-1} \in 1 + m$, so $\omega(a)^{q-1} = 1$, so indeed the image of ω is contained in $\mu_{q-1}(K)$. □

It's easy to see that for $a \in \mu'(K)$, $\omega(a) = a$, so that ω coincides with the multiplicative section $s : (A/m)^\times \to A^\times$ constructed above: let $a \in \mu'(K)$ have order n, and choose N such that $q^N \equiv 1$ (n). Then $a^{q^{jN}} = a$ for all j. In fact this simple observation tells us what we want to know:

Theorem 9. *Let K be a local field with residue field $\mathbb{F}_q = \mathbb{F}_{p^r}$. Then $\mu'(K) = \mu_{q-1}(K)$. That is, the group of roots of unity in K of order coprime to p is naturally isomorphic to the multplicative group of the residue field.*

Proof. Take $\alpha \in \mu'(K)$. Then $\omega(\alpha) = \alpha$, but by Lemma 8, $\omega(\alpha) \in \mu_{q-1}(K)$. □

(What about the p-power roots of unity? It would be nice to prove that $\mathbb{Q}_p(\zeta_p)$ is totally ramified over $\mathbb{Q}_p$ of degree $p-1$. This is a nice application of the connection between totally ramified extensions and Eisenstein polynomials. –PLC2009)

7. Unramified Extensions

Recall that an extension of local fields L/K with corresponding residue extension l/k is unramified if the natural map $G(L/K) \to G(l/k)$ is injective. We use the results of the previous section to characterize the unramified extensions as precisely those which can be obtained by adjoining roots of unity corpime to the residue characteristic. In particular, they correspond bijectively to (arbitrary) extensions of the residue field.

Proposition 10. *Let L/K be a finite extension of local fields generated by roots of unity coprime to p. Then L/K is an unramified cyclic extension.*

Proof. Write $l = \mathbb{F}_q$. Then by hypothesis and Theorem 9 we have $L = K[\mu_{q-1}(L)]$. Thus L is the splitting field of the polynomial $x^{q-1} - 1$ over K, hence Galois. Take $s \in G(L/K)$ and consider $\overline{s} \in G(l/k)$. If $\overline{s} = 1$ on $G(l/k)$, then $s(a) \equiv a \ (m_L)$ for all a in L. Since $\mu_{q-1}(L)$ forms a complete set of coset representatives for $(A_L/m_L)^\times$ and s permutes the elements of $\mu_{q-1}(L)$, we conclude that s fixes every element of $\mu_{q-1}(L)$, hence s is the identity element of $G(L/K)$. That is, $s \to \overline{s}$ is an isomorphism, and $G(L/K) \cong G(l/k)$ is cyclic. □

Conversely, we have the following:

Proposition 11. *Let L/K be a finite, unramified extension of local fields. Then $L = K[\mu_{q-1}(L)]$, where $q = \#l = A_L/m_L$. In particular, there is a unique unramified extension of any local field K of any given finite degree f, and this extension is obtained by adjoining to K the $(q^f - 1)$st roots of unity.*

Proof. Let $K' := K[\mu'(L)]$, so $L/K'/K$ is a tower of local field extensions. By Proposition 10, K'/K is unramified of degree equal to the degree of the residue extension $k[\mu_{q-1}]/k$. But the residue extension of L/K is also $l/k = k[\mu_{q-1}]/k$. Since both extensions are unramified and have the same residual degree, we conclude $[L : K] = [K' : K]$, so $L = K'$, proving the first statement. The second statement follows immedaitely from the elementary fact that a finite field has a unique extension of any given degree. □

To sum up, finite unramified extensions of a local field correspond bijectively to arbitrary extensions of the residue field. Each such extension is cyclic and obtained by adjoining roots of unity coprime to the residue characteristic.

Passage to the limit: Consider K^{unr}, the *maximal unramified extension* of a local field K, i.e. the direct limit (or compositum) of all finite unramified extensions. It follows immediately from the propositions of this section that $K^{\text{unr}} = K[\mu'(\overline{K})]$, i.e. obtained by adjoining all roots of unity of order coprime to p (relative to some fixed algebraic closure $\overline{K}$ of K. Write K_n for $K[\mu_{q^n-1}(\overline{K})]$, the unique unramified extension of degree n. It follows that

$$G(K^{\text{unr}}/K) = \varprojlim G(K_n/K) = \varprojlim G(k_n/k) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

It follows that the absolute Galois group G_K of K is an extension of $\hat{\mathbb{Z}}$, for we have an exact sequence:

$$1 \longrightarrow \mathcal{I} \longrightarrow G_K \longrightarrow \hat{Z} \longrightarrow 1,$$

where $\mathcal{I} = G(\overline{K}/K^{\text{unr}})$ is the *inertia group.* It is easy to see that $\mathcal{I}$ is itself the inverse limit over the inertia subgroups of the finite Galois extensions, hence the name.

8. Ramification Groups

Let L/K be a Galois extension of local fields with Galois group G, with respective valuation rings A_L and A_K. Recall that if the extension is totally ramified, then A_L is a free A_K-module, and if π is a uniformizer for L, then $A_L = A_K[\pi]$ [Serre, Prop. 1.18]. In the general (not necessarily totally ramified) case, we have the following easy result:

Proposition 12. *For $s \in G$ and $i \geq -1$ an integer, the following are equivalent:*
a) s acts trivially on A_L/m_L^{i+1}.
b) $v_L(s(a) - a) \geq i + 1$ for all a in A_L.
c) If x in A_L is such that $A_L = A_K[x]$, then $v_L(s(x) - x) \geq i + 1$.

We write G_i for the set of elements of G satisfying these equivalent conditions. Evidently the G_i form a decreasing sequence of normal (by part *a*)) subgroups of G; moreover $G_{-1} = G$; $G_0 = I$ and $G_i = 1$ for $i \gg 0$. The G_i's are called the *ramification groups* (with lower indexing). Also observe that if we start with an arbitrary extension L/K, then for all $i \geq 0$, the ramification groups are the same as for $G(L/K^{\text{unr}}) = I$, the inertia subgroup.

Proposition 13. *Fix i in $\mathbb{N}$. Let s be an element of G_0. Then s is in G_i if and only if $s(\pi)/\pi \equiv 1(m_L^i)$.*

Proof. Replacing G by G_0 and K by K^{unr} reduces us to the case of a totally ramified extension, in which case, as above, we can write $A_L = A_K[\pi]$. So $v_L(s(\pi) - \pi) = 1 + v_L(s(\pi)/\pi - 1)$, since π is a uniformizer for L. Thus $s(\pi)/\pi \equiv 1 \ (m_L^i)$ iff $v_L(s(\pi)/\pi - 1) \geq i$ iff $v_L(s(\pi) - \pi) \geq i + 1$ iff s is in G_i. □

Filtration on units: Put $U_L^0 := A_L^\times$ and for $i \geq 1$, $U_L^i := 1 + m_L^i$. The U_L^i's give a neighborhood base at 1 for the unit group $A_L^\times = U_L$. Since $A_L^\times$ is closed in the profinite group A_L, it is also profinite, i.e. $A_L^\times = \varprojlim A_L^\times/U_L^i$.

Proposition 14. *a) $U_L^0/U_L^1 = l^\times$.*
b) For $i \geq 1$, $U_L^i/U_L^{i+1} = m_L^i/m_L^{i+1} \cong (l, +)$.

Proof. Indeed we have already used part a) (in the proof of Lemma 8); the identification comes from the natural map $A^\times/(1+m) \to (A/m_L)^\times$. We repeat it here for the purpose of comparison. As for part *b*), to $x \in m_L^i$, associate $1 + x \in U_L^i$. This gives an isomorphism by passage to the quotient, since $1 + x \in U_L^{i+1}$ iff $x \in m_L^{i+1}$. This gives the asserted identification. The isomorphism comes from regarding m_L^i/m_L^{i+1} as an $l = A_L/m_L$-module in the obvious way, and checking that it is one-dimensional over l. Thus, as an abelian group, it is (non-canonically) isomorphic to the additive group of l. □

The following proposition relates the filtrations on G and on U_L:

Proposition 15. *The map $s \mapsto s(\pi)/\pi$ induces by passage to the quotient a monomorphism $\theta_i : G_i/G_{i+1} \to U_L^i/U_L^{i+1}$. The induced map is independent of our choice of a uniformizer π.*

Proof. By Proposition 13, $s(\pi)/\pi$ is in U_L^i and $s(\pi)/\pi \in U_L^{i+1}$ iff $s \in G_{i+1}$, so it is clear that the map is a well-defined monomorphism. To show independence of π, let $\pi' = u\pi, u \in U_L$ be another uniformizer of L, so that $s(\pi')/\pi' = s(\pi)/\pi.s(u)/u$. For $s \in G_i$, $s(u) \equiv u(m_L^{i+1})$, showing that $s(u)/u \in U_L^{i+1}$, showing independence of π upon passage to the quotient. The homomorphism law follows by a similar argument which makes use of the independence of θ_i on a uniformizer: for $s, t \in G_i$,

$$\frac{s(\pi)}{\pi} \cdot \frac{t(\pi)}{\pi} \cdot \frac{\pi}{st(\pi)} = \frac{s(\pi)}{\pi} \cdot \left\{ \frac{s(t(\pi))}{t(\pi)} \right\}^{-1}.$$

But π is a uniformizer iff $t(\pi)$ is a uniformizer, so the expression evaluates to 1 in the quotient. □

Corollary 16. *G_0/G_1 is a cyclic group, and $\theta_0 : G_0/G_1 \hookrightarrow l^\times$. Hence $\#G_0/G_1$ is coprime to p, the characteristic of l.*

Proof. Since $U_L^0/U_l^1 \cong l^\times$, this follows immediately from Proposition 15. □

Corollary 17. *For all $i \geq 1$, G_i/G_{i+1} are abelian groups of exponent p. Further, G_1 is a p-group. $G = G_{-1}$ is itself a solvable group.*

Proof. The map $\theta_i : G_i/G_{i+1} \hookrightarrow m_L^i/m_L^{i+1} \cong (l, +)$, and indeed the additive group of l has expponent p. As for the second statement, we can write $\#G_1 = \prod_{i \geq 1} \#G_i/\#G_{i+1}$ – the product is in fact finite since $G_i = 1$ for all $i \gg 0$, and from this we immediately deduce that the order of G_1 is a power of p. As for the final statement, we have an exact sequence of groups

$$1 \longrightarrow G_1 \longrightarrow G_0 \longrightarrow G_0/G_1 \longrightarrow 1.$$

G_1 is a p-group, hence solvable; by Corollary 16, G_0/G_1 is cyclic, hence solvable, and extensions of solvable groups are solvable, so we conclude that G_0 is solvable. Similarly, $G/G_0 = g(l/k)$ is cyclic hence solvable, and exactly the same argument applies to show that G is solvable. □

9. Tame and Wild Ramification

Let L/K be an extension of local fields, with ramification index $e = \#G_0$. We say L/K is *tamely ramified* if e is coprime to p, the residue characteristic. If on the other hand the ramification index is a power of p, we say L/K is *wildly ramified.* Since G_1 is a p-subgroup of G_0, the following result is immediate:

Corollary 18. *If L/K is tamely ramified, then $G_1 = 1$.*

Back to the general case of a finite Galois extension of local fields: just as in Section 4 we decomposed such an extension into an unramified piece and a totally ramified piece, we can now further decompose the totally ramified piece into tame ramification and wild ramification. That is, we use our exact sequence:

$$1 \longrightarrow G_1 \longrightarrow G_0 \longrightarrow G_0/G_1 \longrightarrow 1.$$

Let us write $\mathcal{P}$ for G_1, I for G_0 (as above) and Δ for G_0/G_1, so our exact sequence now reads

$$1 \longrightarrow \mathcal{P} \longrightarrow \mathcal{I} \longrightarrow \Delta \longrightarrow 1.$$

On the other hand, put $T := G/G_1 = G(L^{\mathcal{P}}/K)$, the maximal tamely ramified subextension of L. We thus get two more exact sequences

$$1 \longrightarrow \mathcal{P} \longrightarrow G \longrightarrow T \longrightarrow 1.$$

$$1 \longrightarrow \Delta \longrightarrow T \longrightarrow g \longrightarrow 1.$$

10. TTR Extensions

Fix a local field K which is *absolutely unramified*, that is, unramified over $\mathbb{Q}_p$, and let $k = \mathbb{F}_q$ be the residue field of K. Let K_n be the unique unramified extension of degree n, i.e. $K_n = \mathbb{Q}_p[\mu_{q^n-1}(\overline{\mathbb{Q}_p})]$. We classify the *totally tamely ramified* (ttr) extensions. If L/K_n is ttr, then $G = G(L/K_n) = G_0$ and $G_1 = 1$, so ramification theory tells us that $G \hookrightarrow l^\times = k_n^\times$, where the residue fields of L and K_n coincide since the extension is totally ramified. It follows that if we can find an extension with $G(L/K_n) = k_n^\times$, it must be the (unique) maximal ttr extension. But we can construct such an extension very explicitly: put $L := K_n^{tr} := K_n[X]/(X^{q^n-1} - p)$. Since $K_n/\mathbb{Q}_p$ is unramified, $X^{q^n-1} - p$ is Eistenstein at p, hence irreducible. Therefore the degree of L/K is $q^n - 1$, which is coprime to p, so the extension is tamely ramified; on the other hand, L/K_n is quite visibly totally ramified, therefore L/K is ttr. This is one case in which it is easy to compute the Galois group $G(L/K_n)$ by hand: let α be choice of a $(q^n - 1)$st root of p in L, so the conjugates of α are just $\alpha \cdot \zeta^i, 0 \leq i \leq q^n - 1$, where ζ is a primitive $(q^n - 1)$st root of unity, which, recall, lies in K_n by assumption. This confirms that L/K_n is Galois, and clearly all the automorphisms are of the form $\alpha \mapsto \alpha \cdot \zeta^i$, so L/K_n is cyclic of degree $q^n - 1$. Since $k_n^\times$ is also a cyclic group of that order, we have an abstract group isomorphism $G(L/K_n) \cong k_n^\times$, which is enough to see that L is the maximal ttr extension of K.

However, we want to *canonically* identify $G(L/K_n)$ with $k_n^\times$, and later on we will need the stronger statement that the two are isomorphic as $G(K_n/K)$-modules. Here $k_n^\times$ has an obvious $G(K_n/K) = g(k_n/k)$-module structure, and $G(L/K_n)$ gets its $G(K_n/K)$-action via the group extension

$$1 \longrightarrow G(L/K_n) \longrightarrow G(L/K) \longrightarrow G(K_n/K) \longrightarrow 1.$$

More explicitly, given an element of $G(K_n/K)$, we lift it to any element of $G(L/K)$ and have that element act on the normal subgroup $G(L/K_n)$ by conjugation. Since $G(L/K_n)$ is abelian, this action is independent of the lift.

The isomorphism is an application of Kummer Theory: let $\rho : \overline{K_n}^\times \to \overline{K_n}^\times$ be the map $x \mapsto x^{q^n-1}$. The kernel of the map is the group of $(q^n - 1)$st roots of unity in $\overline{K_n}^\times$, which we may canonically identify with $k_n^\times$. Thus we have a short exact sequence of $G(\overline{K_n}/K)$-modules:

$$1 \longrightarrow k_n^\times \longrightarrow \overline{K_n}^\times \xrightarrow{\rho} \overline{K_n}^\times \longrightarrow 1.$$

Applying Galois cohomology and using Hilbert 90 we get

$$K_n^\times / K_n^{\times q^n-1} \cong H^1(G_{K_n}, k_n^\times) = \mathrm{Hom}(G_{K_n}, k_n^\times).$$

Consider the image of p in the left-hand side; it has order $q^n - 1$. Under the isomorphism p corresponds to the map $\phi : \sigma \mapsto \sigma(\alpha)/\alpha$. (This formula for the isomorphism comes from writing down the coboundary map in the long exact cohomology sequence.) The kernel of ϕ is precisely $G(\overline{K_n}/L)$, so ϕ yields the *explicit* isomorphism

$$G(L/K_n) = G(\overline{K_n}/K_n)/G(\overline{K_n}/L) \xrightarrow{\sim} k_n^\times$$

that we wanted. Moreover, it's easy to see that the Kummer isomorphism respects the $G(K_n/K)$-action on both sides: after applying cohomology, all the terms have $G(K_n/K)$-module structure, and the only thing to check is that the coboundary map respects that structure.

$\mathbf{T_n}$: As above, we can compile the tamely ramified and the unramified pieces into an extension whose Galois group is still easy to calculate explicitly. (Conversely, the remaining, wildly ramified piece is a p-group that is much more complicated.) Write $T_n := G(L/K)$, where K is still a local field that is absolutely unramified over $\mathbb{Q}_p$. We have an exact sequence

$$1 \longrightarrow k_n^\times \longrightarrow T_n \longrightarrow g_n = g(k_n/k) \longrightarrow 1.$$

We claim the sequence *splits*, giving a semidirect product decomposition $T = k_n^\times \rtimes g_n$. Indeed, it's enough to produce a multiplicative section $s : G(K_n/K) \hookrightarrow G(L/K)$, and we can do this explicitly by extending the automorphism $\zeta \mapsto \zeta^{q^i}$ to $\zeta \mapsto \zeta^{q^i}, \alpha \mapsto \alpha$, which works. Thus we have computed the Galois group of the tamely ramified piece of any finite extension L/K, K an absolutely unramified local field. We can even get a presentation for $G(L/K)$ in terms of generators and relations: let ϕ be a lift of the Frobenius automorphism of $G(K_n/K)$ to $G(L/K)$, i.e. $\phi : \zeta \mapsto \zeta^q, \alpha \mapsto \alpha$; let τ be a generator of $G(L/K_n)$, so $\tau : \zeta \mapsto \zeta, \alpha \mapsto \alpha\zeta$. Then one checks easily that $G(L/K) =$
$< \ \phi, \tau | \ \phi^n = 1, \tau^{q^n-1} = 1, \phi\tau\phi^{-1} = \tau^q >$. We can see this is another way using the fact that $G(L/K_n)$ and $k_n^\times$ are isomorhphic as $G(K_n/K)$-modules: the action of ϕ on $G(L/K_n) = k_n^\times$ is on the one hand given by conjugation and on the other hand given by the Frobenius map.

Passage to the limit: We now take $K = \mathbb{Q}_p$ and consider what happens upon passage to the limit. Let $\mathbb{Q}_p^{\mathrm{tame}}$ be the direct limit of all the tamely ramified extensions. Certainly $\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}$ is Galois and has $\mathbb{Q}_p^{\mathrm{unr}}$ as a subextension. Moreover, it follows from our analysis of the finite case that $G(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p^{unr})$ is the inverse limit of the Kummer extensions L_n/Q_p^{unr} obtained by adjoining (p^n-1)st roots of p. Here the defining maps of the inverse limit are the natural surjections $G(L_{nn'}/\mathbb{Q}_p^{\mathrm{unr}}) \to G(L_n/\mathbb{Q}_p^{\mathrm{unr}})$. Under the canonical isomorphism provided by Kummer theory, one can easily check that these correspond to the *norm maps* $N : k_{nn'}^\times \mapsto k_n^\times$ (in particular, this is one of many ways to see that the norm map on an extension of finite fields is surjective). Group-theoretically, we are getting an inverse limit over all cyclic groups of p'-order via surjective maps. One can check that any such inverse limit is isomorphic (very non-canonically) to $\prod_{l \neq p} \mathbb{Z}_l =: \Delta_p$. (More accurately, we should write $\Delta_p = \prod_{l \neq p} \mathbb{Z}_l(1)$ to emphasize that the Galois action of $g = G(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p)$ on Δ_p is not the trivial action, but rather the Tate-twisted action on the roots of unity.) In particular, for $T := G(\mathbb{Q}_p^{\mathrm{tame}}/\mathbb{Q}_p)$, we have an exact sequence

$$1 \longrightarrow \Delta_p \longrightarrow T \longrightarrow \hat{Z} \longrightarrow 1.$$

As in the finite case, we can lift the generator (Frobenius) ϕ of $\hat{Z}$ to an element of T and use it to act on the procyclic group Δ_p, so the inverse limit T retains the semidirect product decomposition $T = \Delta_p \rtimes_\phi \hat{Z}$.

Finally, it is natural to ask for the profinite analogue of the presentation obtained for T_n above. On the one hand, since in passing to the limit we are allowing the generators ϕ and τ to have larger and larger order while the conjugation relation $\phi\tau\phi^{-1} = \tau^p$ holds independently of n, it's natural to believe that T should have something to do with the group $\mathfrak{T} =< \phi, \tau \mid \phi\tau\phi^{-1} = \tau^p >$. But, since $\mathfrak{T}$ is a countably infinite group, it has no chance of being a profinite group in any topology. So the most we can hope for is that T is the profinite completion of $\mathfrak{T}$, which indeed turns out to be the case.

Proposition 19. *$T = \hat{\mathfrak{T}}$, the profinite completion of $\mathfrak{T}$.*

Proof. Observe that the presentation of $\mathfrak{T}$ gives rise to an internal semidirect product decomposition $\mathfrak{T} = \langle\tau\rangle \rtimes \langle\phi\rangle$. Taking the profinite completion, we get a semidirect product decomposition $\hat{\mathfrak{T}} = \widehat{\langle\tau\rangle} \rtimes \widehat{\langle\phi\rangle}$. We can compute these two profinite groups. The closure of $\langle\phi\rangle$ in $\hat{\mathfrak{T}}$ is $\hat{\mathbb{Z}}$, since the relations $\phi\tau\phi^{-1} = \tau^p, \phi^n = \tau^n = 1$ yield no further restrictions on words in ϕ alone. On the other hand, consider the closure of $\langle\tau\rangle$ in $\hat{\mathfrak{T}}$. The conjugation relation $\phi\tau\phi^{-1} = \tau^p$ enforces the condition that p be coprime to the order of the image of τ in any finite quotient, so the closure of $\langle\tau\rangle$ is precisely the inverse limit of all cyclic groups of p'-order, i.e. Δ_p. Hence the exact sequence associated to the semidirect product decomposition reads

$$1 \longrightarrow \Delta_p \longrightarrow \hat{\mathfrak{T}} \longrightarrow \hat{\mathbb{Z}} \longrightarrow 1.$$

But the conjugation relation $\phi\tau\phi^{-1} = \tau^p$ determines the action of $\hat{\mathbb{Z}}$ on Δ_p: it is via the pth-power Frobenius map. Thus $\hat{\mathfrak{T}} = \Delta_l \rtimes_\phi \hat{\mathbb{Z}}$, i.e. precisely the same semidirect product decomposition as for T. □

11. Decomposition of the Absolute Galois Group

In this final section we restate our results in terms of a "decomposition" of the absolute Galois group of a local field. Since by definition T is the maximal totally tamely ramified quotient of $G_{\mathbb{Q}_p}$, we have an exact sequence

$$1 \longrightarrow \mathcal{P} \longrightarrow G_{\mathbb{Q}_p} \longrightarrow T \longrightarrow 1,$$

where $\mathcal{P}$ is the inverse limit over the wildly ramified subgroups of the finite Galois extensions of $\mathbb{Q}_p$, hence is a (very complicated) pro-p subgroup. We summarize our analysis of $G_{\mathbb{Q}_p}$ in the following diagram:

Finally, let $K/\mathbb{Q}_p$ be an arbitrary finite extension of local fields. We have a natural embedding $G_K \longrightarrow G_{\mathbb{Q}_p}$ which we can use to study the structure of G_K. Put $\mathcal{I}_K := \mathcal{I} \cap G_K, \mathcal{P}_K := \mathcal{P} \cap G_K$. Then $\mathcal{I}_K$ is just the inertia group of $\overline{K}/K$. We also put $T_K :=$ the image of G_K under the natural map $G_{\mathbb{Q}_p} \to T$. Note well that if $K/\mathbb{Q}$ is wildly ramified, then T_K is *not* equal to the tame inertia group of K in the absolute sense. Instead, define $T_{e,f}$ for positive integers e and f to be the (closed, finite index) subgroup of $T_{\mathbb{Q}_p}$ generated by τ^e and ϕ^f, and let e' be the

p'-component of $e(K/\mathbb{Q}_p)$ and f be the residue degree of $K/\mathbb{Q}_p$. Then one can check that $T_K = T_{e,f}$, and we have an exact sequence

$$1 \longrightarrow \mathcal{P}_K \longrightarrow G_K \longrightarrow T_K \longrightarrow 1.$$